(12) PATENT ABSTRACT (11) Document No AU-A-59440/98
(19) AUSTRALIAN PATENT OFFICE

(54) Title
A RISK BASED CONTROL SYSTEM

International Patent Classification(s)
(51)° **G06F 017/60**

(21) Application No : **59440/98** (22) Application Date **20/03/98**

(30) Priority Data

(31) Number	(32) Date	(33) Country
PO6788	20/03/97	AU AUSTRALIA

(43) Publication Date : **24/09/98**

(71) Applicant(s)
BERGMAN VOYSEY & ASSOCIATES PTY LIMITED

(72) Inventor(s)
NAME NOT GIVEN.

(74) Attorney or Agent
F B RICE & CO , 605 Darling Street, BALMAIN NSW 2041

(57) Claim

1. A method of using a computer equipped with a relational database to provide control output to address the threats confronting a system or organisation, comprising the steps of:

creating a series of relational database entities which describe the system;

analysing the system to derive data relevant to the entities; and

reporting from the database to produce the control output;

wherein the entities and data concern the following:

the objectives of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the processes of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the resources used to perform the processes;

the locations, persons and positions involved with the objectives processes and resources;

the risks those processes and resources are subject to;

the consequences should those risks materialise;

the controls which mitigate the risks; and

assessments;

each combination of objective, process and risk linked to the consequence, resource, control and recommendation entities;

and wherein:

the analysis involves the use of the combinations of objective, process and risk, reporting involves a link between the consequences and

.../2

assessment entities;
and

the control output includes a list of the exposures and scenarios which have an unacceptable risk associated with them.

AUSTRALIA

Patents Act 1990

BERGMAN VOYSEY & ASSOCIATES PTY LIMITED

ORIGINAL

COMPLETE SPECIFICATION
STANDARD PATENT

Invention Title:

A risk based control system

The following statement is a full description of this invention including the best method of performing it known to us:

Technical Field

This invention concerns a method using a computer to provide risk based control output. In another aspect it concerns a computer system for use in risk based control.

Background Art

Risk is measured in terms of the likelihood and consequence of an occurrence taking into consideration existing control measures. Risk management is an interactive process consisting of well-defined steps which, taken in sequence, support better decision-making by contributing a greater insight into risks and their impacts. Risk management can be applied to any situation where an organisation or system can minimise losses or maximise opportunities.

Risk may arise from internal or external sources. Both sources of risk need to be considered when identifying risk. Causes of risk include the following:

Natural (Delay, Interruption, Loss) - includes earthquake, lightning strike, storm, flood and drought.

Unintentional Human Behaviour (Substandard Quality) - includes error, omission and accident.

Intentional Human Behaviour (Unauthorised Acts) - includes fraud, theft, riot and sabotage.

Other sources of risk include:

Technological - includes obsolescence, advances and failure.

Economic and Financial - includes international exchange rates and domestic factors such as interest rates and unemployment.

Environmental - includes noise, contamination and pollution.

Commercial and Legal - includes liability and other contractual obligations.

Statutory - includes censure, fine, disallowance and jail sentence.

Political - includes legislative change, public perception and image.

Management of risk is an integral part of the management process.

Risk management is an iterative process comprising six main elements or steps as follows:

Establish the context - This step establishes the strategic, organisational and risk management context in which the rest of the process

will take place. Criteria against which risk will be assessed are established and the structure of the analysis is defined.

Identify risks - Identify what, why and how things can arise as the basis for further analysis.

Analyse risks - Determine the existing management controls and analyse risk in terms of likelihood and consequence in the context of those controls. The analysis considers:

(i) how likely is an event to happen and

(ii) what are the potential consequences and their magnitude?

These elements are then combined to produce an estimated level of risk.

Evaluate risks - Compare estimated levels of risks against the pre-established criteria. Risk are then ranked to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.

Treat risks - Accept and monitor low priority risks. For other risks developed and implemented a specific management plan which includes consideration of funding.

Monitor and review - Monitor and review the performance of the risk management system and changes which might affect it.

The risk management process has traditionally involved a more or less systematic collection of data and subsequent analysis by an experienced professional to produce a report.

Summary of the Invention

The present invention is a method of using a computer equipped with a relational database to provide control output to address the threats confronting a system or organisation, comprising the steps of:

creating a series of relational database entities which describe the system;

analysing the system to derive data relevant to the entities; and

reporting from the database to produce the control output;

wherein the entities and data concern the following:

the objectives of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the processes of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the resources used to perform the processes;

the locations, persons and positions involved with the objectives processes and resources;

the risks those processes and resources are subject to;

the consequences should those risks materialise,

the controls which mitigate the risks, and

assessments;

each combination of objective, process and risk linked to the consequence, resource, control and recommendation entities;

and wherein:

the analysis involves the use of the combinations of objective, process and risk, reporting involves a link between the consequences and assessment entities; and

the control output includes a list of the exposures and scenarios which have an unacceptable risk associated with them.

This provides the advantages that:

Management is able to identify those functions or processes within a system, such as an organisation, which are dependent on specific resources and the risks which those functions and resources are subject to.

Risk are evaluated in terms of likelihood and consequence.

Management is able to identify the most at risk functions and resources.

Risks can be avoided, transferred in part or in full, or mitigated by instituting additional controls to lower the likelihood or consequences or both likelihood and consequence.

Risks can be properly managed and insurance risk financing costs kept to a minimum.

In another aspect the invention, as currently envisaged, is a computer system for providing control output to address the threats confronting a system or organisation, comprising:

a computer equipped with a data input means, a data processor and a relational database in which there are created a series of relational database entities which describe the system;

wherein the entities and data concern the following:

the objectives of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;
the processes of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;
the resources used to perform the processes;
the locations, persons and positions with the objectives processes and resources;
the risks those processes and resources are subject to;
the consequences should those risks materialise;
the controls which mitigate the risks; and
assessments,

each combination of objective, process and risk linked to the consequence, resources, control and recommendation entities; and wherein the processor accesses the relational database, analyses data relevant to the entities using the combinations of objective, process and risk, and reports the control output using a link between the consequence and assessment entities to produce a list of the exposures and scenarios which have an unacceptable risk associated with them.

Brief Description of the Drawings

An example of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a computer embodying the invention; and

Figure 2 is schematic diagram of a relational database used by the invention.

Best Mode of the Invention

Referring first to figure 1, the computer 1 comprises a data processor 2, data input means 3 and a monitor 4. In addition there is a relational database 5 and a printer 6.

The entities within the relational database 5 and their relationships with each other are shown in more detail in Figure 2. Before a system can effectively be controlled, it is necessary to establish a number of elements of data relating to the entities of the system, for instance the system or

organisation 10, the organisation levels 11, person 12, position 13, location 14 and process 15.

Organisation levels 11 refer to the level of analysis and reporting required for the project, for example the process, division or branch. Normally this is dictated by the structure of the organisation 10 and the amount of analysis required. Each process 15 of the system is assigned an organisation level.

Person 12 details are recorded on the system to identify the people who occupy positions 13 referred to in the system.

Position 13 details are recorded on the system to identify the positions or roles, of the people 12 in the organisation 10. These also identify the responsibilities for processes 15, resources 16, achievement of objectives 17 and implementation of recommendations 26.

Location 14 details are recorded on the system to identify the location of the organisation 10 and its processes 15, positions 13 and resources 16.

The system maintains objective entities 17 which describe the specific corporate vision, missions, corporate goals, strategies, and tactics. Objectives 17 are particularly relevant when risks 18 are assessed at a strategic level.

A process 15 may be a group of tasks, a section of a department, a department, a division or an organisation as a whole. The processes are arranged in a hierarchy whereby sub-processes are linked to any given process of which is part.

Risks 18 identified for assessment are recorded in the system. These could be exposures or scenarios.

The analysis 19 of risks 18 is usually performed in the context of the objectives 17 and processes 15. The combinations 20 of the objectives, processes, and risks are maintained as an entity in the system. Risks are assessed 19 in the terms of their likelihood of occurrence, their worst case impact and their overall loss control. They may also have an estimated maximum potential loss quantitatively recorded.

Risks can be assessed 19 at a strategic level, operational level or specifically for business interruption. When risks are assessed at a strategic level, the importance of the objective 17 is also considered.

In the identification and analysis of risks, their consequences 22 are recorded in the system. Each consequence 22 is linked to an assessment 19.

This link is essential to describe the outcome of an event happening. It also enables the calculation of maximum potential loss.

Resources 16 are required to perform a process 15. Resources include people, systems whether manual or computerised, information and capital assets. Key resources of a process are assessed 23 as to the process's level of dependence on these resources, the probability of losing the resource and the adequacy of its backup/risk control.

Controls 24 are policies, standards and procedures to prevent, detect or correct the consequences of risk. The effectiveness 21 of controls in the context of the objective, process and risk combinations 20 and the resources 16 are established to determine the level of risk. Any control which is not adequate will require treatment. This treatment or corrective action is recorded as a recommendation 26. The recommendation holds information relating to the priority for corrective action, costs, the start and end date (estimated and actual), and the position 13 responsible for implementation.

To prioritise risks, the system calculates the level of risk by taking into account the assessments of likelihood, impact and control, and where applicable, the importance factor of the objective or the level of dependence on a resource.

Example of using the system

The Total Personnel Services Company is a computer payroll services bureau. The company has three divisions:

finance/administration division;
marketing division; and
payroll services division.

The Company's objectives include:

being the leading provider of payroll services which it hopes to accomplish by:

- capturing 90% of the market by 1999;
- providing quality services to its clients; and
- providing an excellent work environment.

The risk scenarios for Total Personnel Services include:

business interruption;
delay interruption loss;
errors and omissions;
failure to achieve objective;

fire;
flood/water damage; and
contractual liability.

The processes for the Payroll Services Division include:

client liaison;
computer operations; and
computer programming.

The key resources required by the Payroll Services Division to perform its processes include:

PC Pay System
PC Server/Terminals/Printer
Key Personnel
Office Facilities.

Each objective is assessed as to its operational risk, strategic risk and combined risk. A raw score and an average score are calculated as follows:

			Objective < All >	Level	All Levels			Operational	1	Strategic	1	Scoring Both
Objective	Level	Objective Importance	Objective Description			Raw Score				Average Score		
				Operational	Strategic Risk Factor	Combined Risk Score		Operational	Strategic Risk Factor		Combined Risk Score	
Obj 2	1	0.25	To capture 10% of the market by 1999	0.20	0.10	0.15		0.20	0.10		0.15	
Obj 3	1	0.5	To provide quality services to clients at the least possible cost	0.20	0.10	0.15		0.20	0.10		0.15	
Obj 4	1	0.25	To provide an excellent working environment for all staff.	0.20	0.10	0.15		0.20	0.10		0.15	
				Total	0.60	0.28	0.44					

The consequences and comment details are then entered and linked to produce a report which shows the linked processes, risk scenario and consequences and where applicable a total value and an impact

Level	Process ID	Process Name Risk Scenario	Sequence ID Consequence	Comment	Included	Comment Value Type	Cost	Max Days	Total Value	Impact
7	Client Loss	Client Location		Pay Secy						
		[illegible]	5	Estimated loss of property equipment	•	[illegible]				
		[illegible]	16	Increased costs	•	[illegible]				
		[illegible]	20	Loss of goodwill/image	•	[illegible]				
		[illegible]	8	Client contact and co-ordination	•					
		[illegible]	10	Unlikely to achieve client operation to ensure deadlines met	•					
		[illegible]	10	Unlikely to achieve client operation to ensure deadlines met	•					
		[illegible]	10	Unlikely to achieve client operation to ensure deadlines met	•					
8	Comp Ops	Computer Operations		Pay Secy						
		[illegible]	15	Estimated loss of property equipment	•	[illegible]				
		[illegible]	17	Estimated loss of staff productivity	•	[illegible]				
		[illegible]	11	Unable to data entry personnel and produce report	•					
9	Comp Prog	Computer Programming		Pay Secy						
		[illegible]	5	Estimated loss of property equipment	•	[illegible]				
		[illegible]	18	Increased costs of temporary	•					
		[illegible]	12	Co-ordination, time of further development/enhancement	•					

The key resources are then assessed as to the dependency of the Payroll Services processes on them, the likelihood of the resources being lost or becoming unavailable, the status of backup risk control and the priority for business recovery planning.

Once assessed, a number of reports can be produced. One of these reports is the Key Resources at Risk report which shows

resource descriptions

functions or processes which use the resource

level of dependence, likelihood, and backup risk control

calculated financial risk factors, dependency risk factors and business recovery planning priority factors expressed in currency or as a percentage

The key controls which mitigate (prevent, detect or correct) the consequences of the risk are then entered into the system against each resource and exposure. These are assessed as to its current effectiveness to mitigate the risk. Where the control is not effective (ie "borderline" or "inadequate" or "non-existent"), the corrective action is also recorded

A number of reports can be produced from the system. These include:

(i) A Risk Mitigation Report which shows

processes and related exposures, resources and consequences with calculated likelihood, impact, control, estimated maximum potential loss, calculated level of risk or residual risk and estimated costs.

(ii) Workpaper of Key Controls, Risk Assessment and Corrective Action which shows:

processes and related exposures and resources with calculated likelihood, impact, control, corrective action priority, position responsible to implement and estimated and actual costs.

(iii) Consequences of Interruption - overview of key processes grouped by level by process, which shows

resources used by each process and sub-process with the critical period the resource is required for

the daily and maximum cost of working without the resource

the estimated time to restore the resource,
the estimated loss of market or revenue,
the estimated loss of property or equipment,
the calculated maximum potential loss (MPL), the individual MPL of each process, and financial risk factors in currency and as a percentage.

Although the invention has been described with reference to a business organisation and the problems of managing that organisation it should be appreciated that the invention could have application to other kinds of systems. For instance, the invention could be applied to the maintenance of sophisticated piece of machinery such as a power station. The objectives in this case might be to maintain production within a specified range, and the risks might include breakdown of particular items of equipment. The control output might be the provision of service reports, and the invention could automatically switch to auxiliary equipment when the risk of continued operation of any piece of equipment becomes too high.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:-

1. A method of using a computer equipped with a relational database to provide control output to address the threats confronting a system or organisation, comprising the steps of:

creating a series of relational database entities which describe the system;

analysing the system to derive data relevant to the entities; and

reporting from the database to produce the control output;

wherein the entities and data concern the following:

the objectives of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the processes of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;

the resources used to perform the processes;

the locations, persons and positions involved with the objectives processes and resources;

the risks those processes and resources are subject to;

the consequences should those risks materialise;

the controls which mitigate the risks; and

assessments;

each combination of objective, process and risk linked to the consequence, resource, control and recommendation entities;

and wherein:

the analysis involves the use of the combinations of objective, process and risk, reporting involves a link between the consequences and assessment entities;

and

the control output includes a list of the exposures and scenarios which have an unacceptable risk associated with them.

2. A computer system for providing control output to address the threats confronting a system or organisation, comprising:

a computer equipped with a data input means, a data processor and a relational database in which there are created a series of relational database entities which describe the system;

wherein the entities and data concern the following:

the objectives of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;
the processes of the system arranged in hierarchies and are each labelled to identify their position in the hierarchy;
the resources used to perform the processes;
the locations, persons and positions with the objectives processes and resources;
the risks those processes and resources are subject to;
the consequences should those risks materialise;
the controls which mitigate the risks; and
assessments;
each combination of objective, process and risk linked to the consequence, resources, control and recommendation entities;
and wherein the processor accesses the relational database; analyses data relevant to the entities using the combinations of objective, process and risk; and reports the control output using a link between the consequence and assessment entities to produce a list of the exposures and scenarios which have an unacceptable risk associated with them.

3. A method of using a computer equipped with a relational database to provide control output to address the threats confronting a system or organisation substantially as described with reference to the drawings and example.

4. A computer system for providing control output to address the threats confronting a system or organisation substantially as described with reference to the drawings and example.

Dated this 20th day of March 1998

BERGMAN VOYSEY & ASSOCIATES PTY LIMITED
Patent Attorneys for the Applicant:

F.B. RICE & CO.

ABSTRACT

This invention concerns a method using a computer to provide risk based control output. In another aspect it concerns a computer system for use in risk based control. Both the method and system require a relational database to provide control output to address the threats confronting a system or organisation. A series of relational database entities which describe the system are created. The system is analysed to derive data relevant to the entities, the analysis involves the use of the combinations of objective, process and risk. A report is obtained from the database to produce a control output, the report involves a link between the consequences and assessment entities. The control output includes a list of the exposures and scenarios which have an unacceptable risk associated with them.

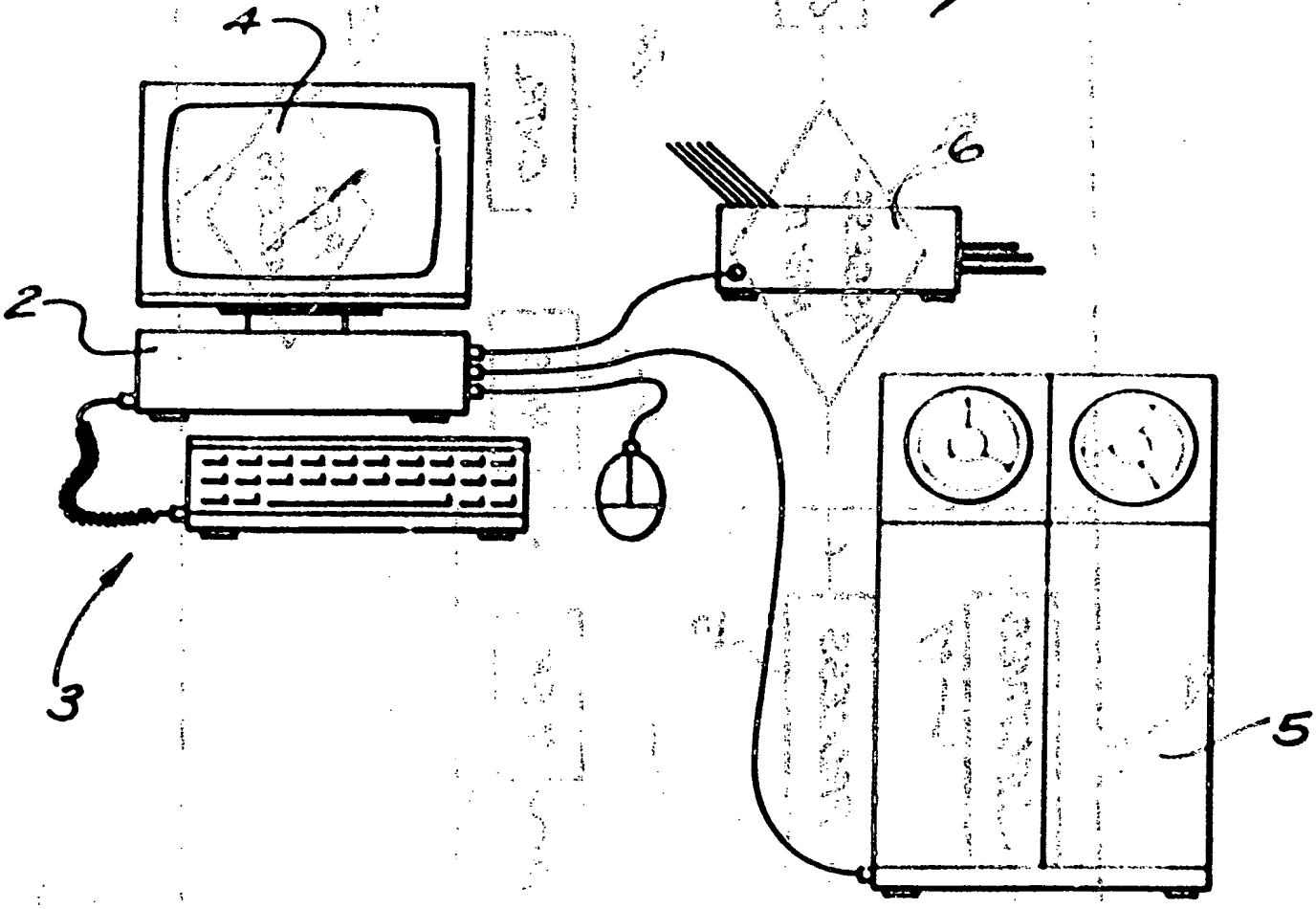

FIG. 1

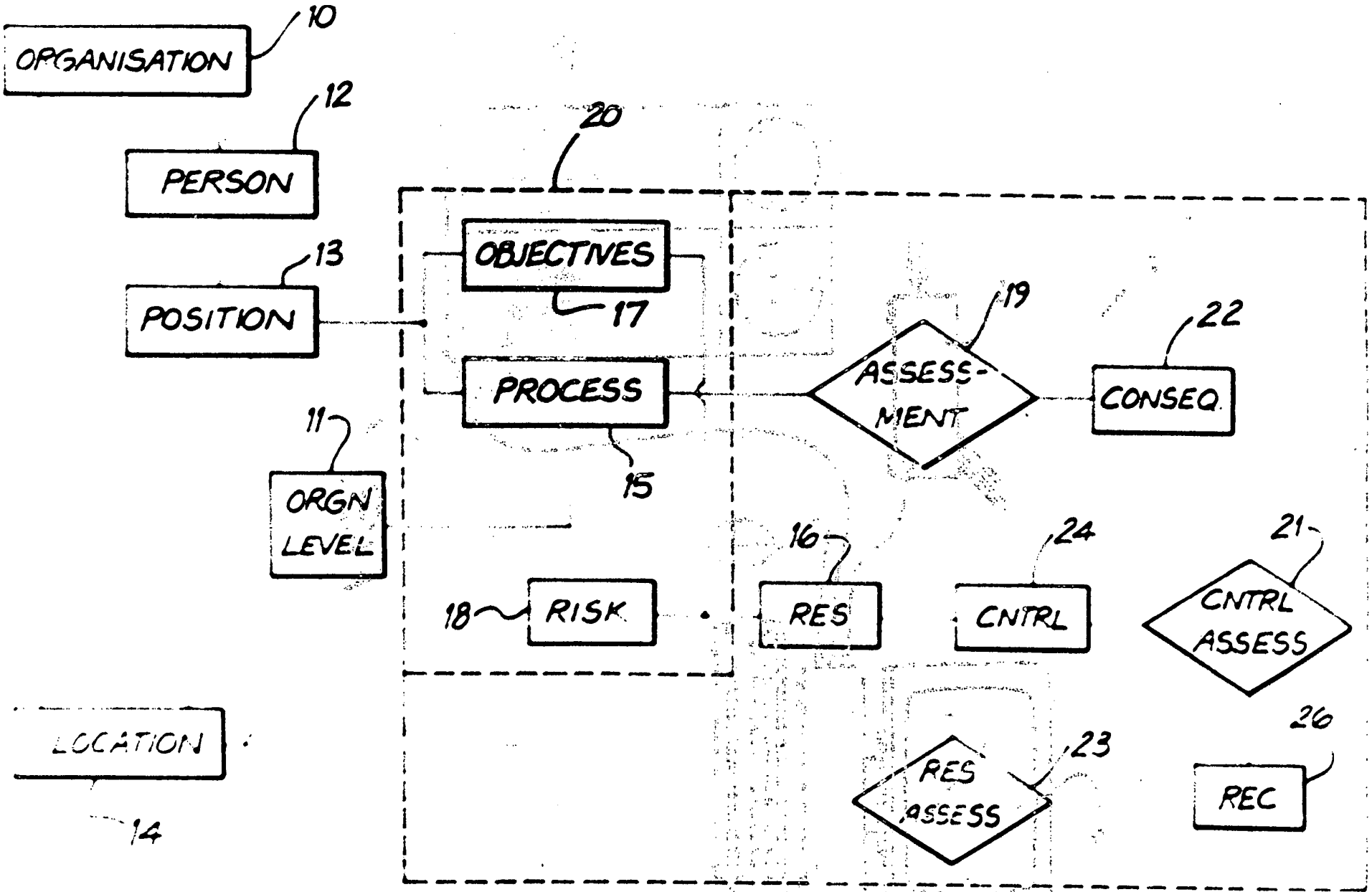
ORGANISATION
10
PERSON
12
POSITION
13
LOCATION
14
20
OBJECTIVES
17
PROCESS
15
11
ORGN LEVEL
18
RISK
19
ASSESS-MENT
22
CONSEQ.
16
RES
24
CNTRL
21
CNTRL ASSESS
RES ASSESS
23
26
REC

FIG. 2